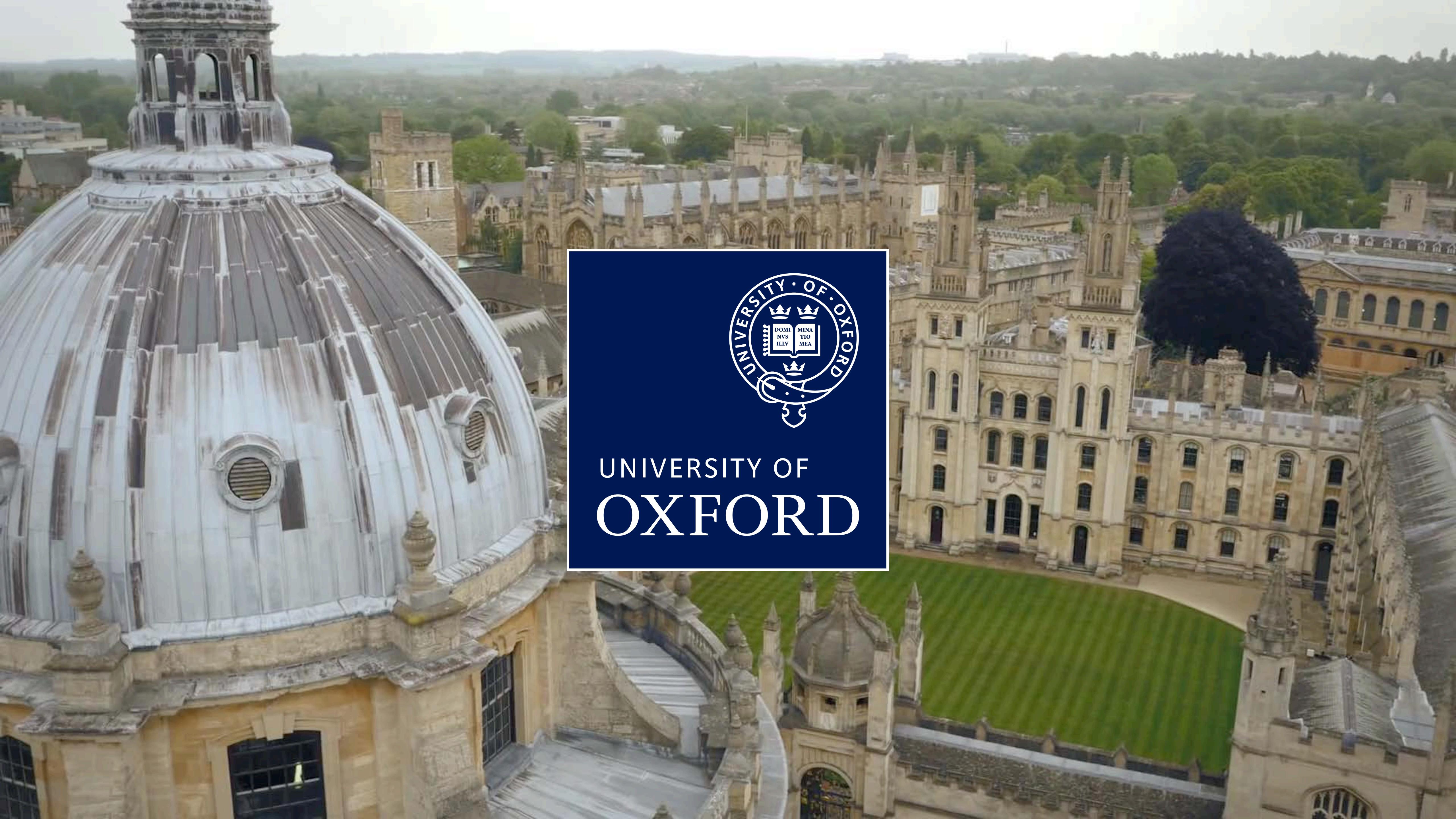
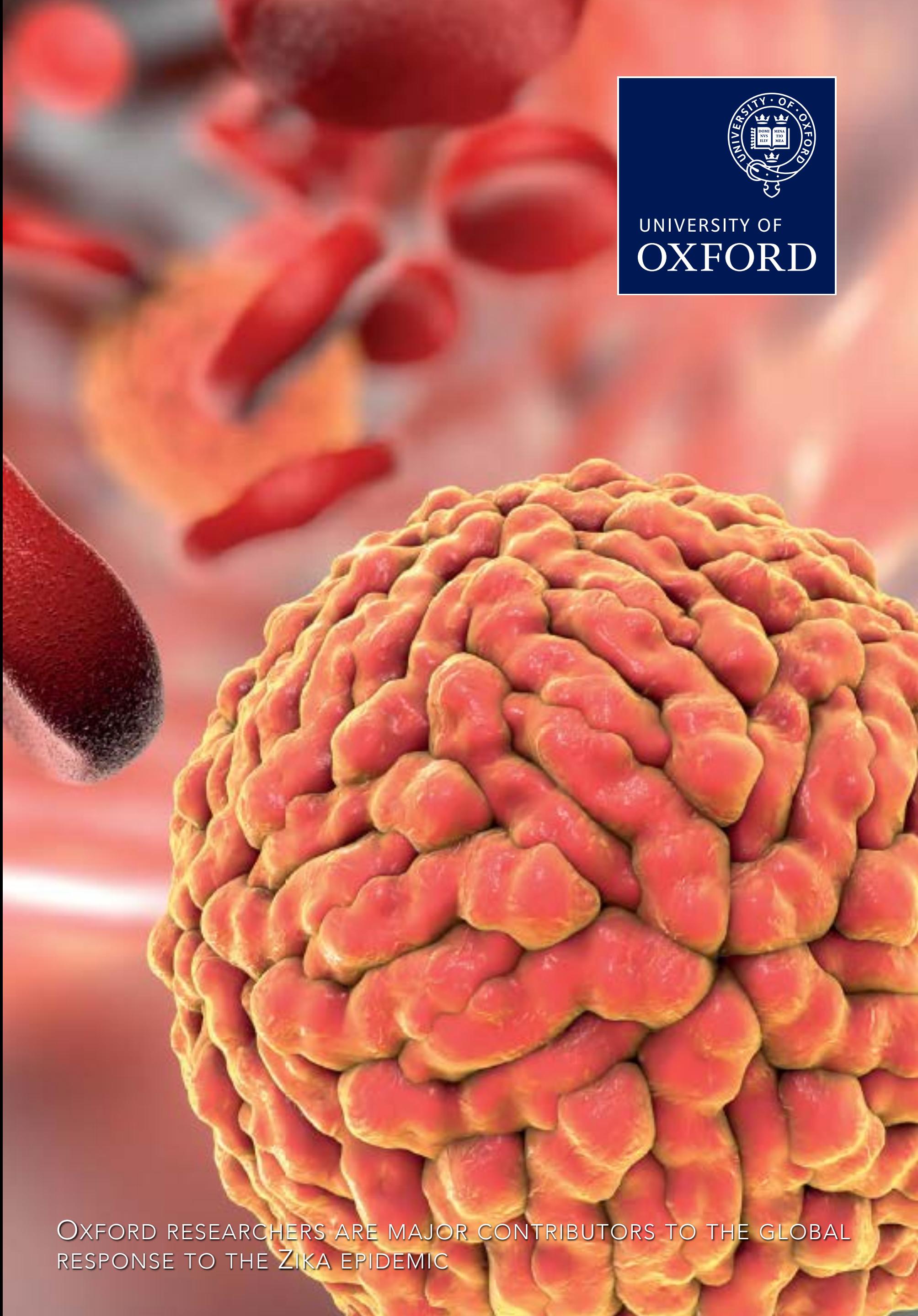


CLOUDSEC2019



# OXFORD RESEARCH

- Oxford employs over 13,900 people, of which 7,260 are academics, researchers or teachers (56%).
- According to the 2014 Research Excellence Framework, the latest official UK-wide assessment of all university research, Oxford has the largest volume of world-leading research in the country.
- 5% of all the UK's graduate research students are studying at the University of Oxford.



OXFORD RESEARCHERS ARE MAJOR CONTRIBUTORS TO THE GLOBAL  
RESPONSE TO THE ZIKA EPIDEMIC

# OXFORD EDUCATION

- Oxford was ranked first in the world in the Times Higher Education (THE) World University Rankings for 2017, 2018, 2019, and 2020.
- Nearly 24,000 students (11,747 UG, 11,687 PG)
- Oxford is very competitive: around 21,500 people applied for around 3,300 undergraduate places for entry in 2018.
- Oxford offers more than 300 different graduate degree programmes.
- 43% of our total student body – almost 10,000 students – are citizens of foreign countries. Students come to Oxford from over 150 countries and territories.



OXFORD STUDENTS CELEBRATING AT RADCLIFFE CAMERA SQUARE  
AFTER THEIR FINAL EXAMS.

# OXFORD INFORMATION TECHNOLOGY

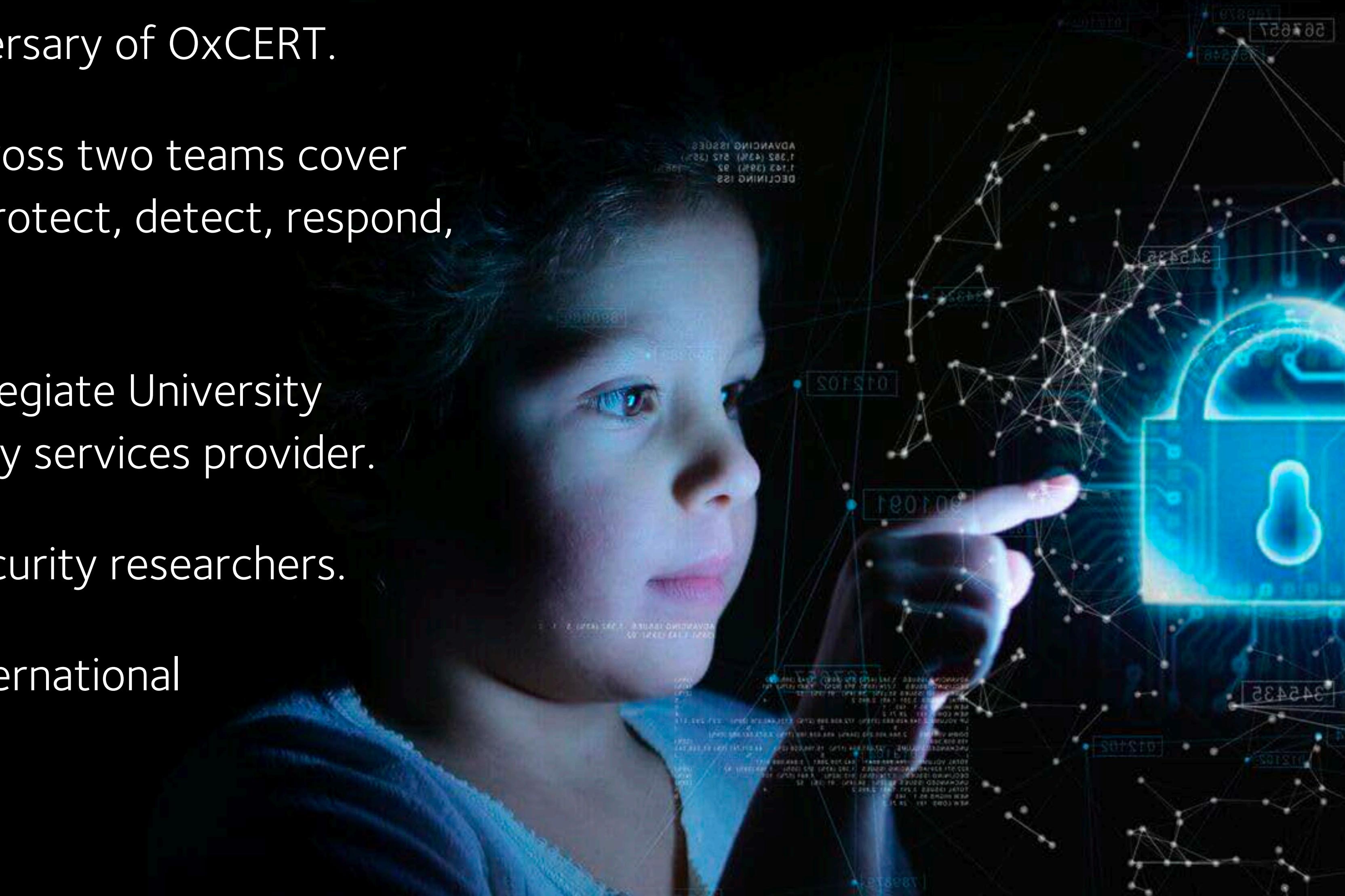
- Highly federated environment with 800 members of IT staff across over 110 units, plus 44 Colleges and Permanent Private Halls.
- Units operate largely independently
- Oxford operates one of the largest private networks in the country with
  - ~100,000 registered devices
  - redundant 40Gbit/s Internet uplink



# OXFORD CYBER SECURITY



- 2019 marks the 25<sup>th</sup> anniversary of OxCERT.
- 17 security experts split across two teams cover all five functions: identify, protect, detect, respond, and recover.
- Offering services to the collegiate University similar to a managed security services provider.
- Collaboration with cyber security researchers.
- Deeply integrated in the international security community.

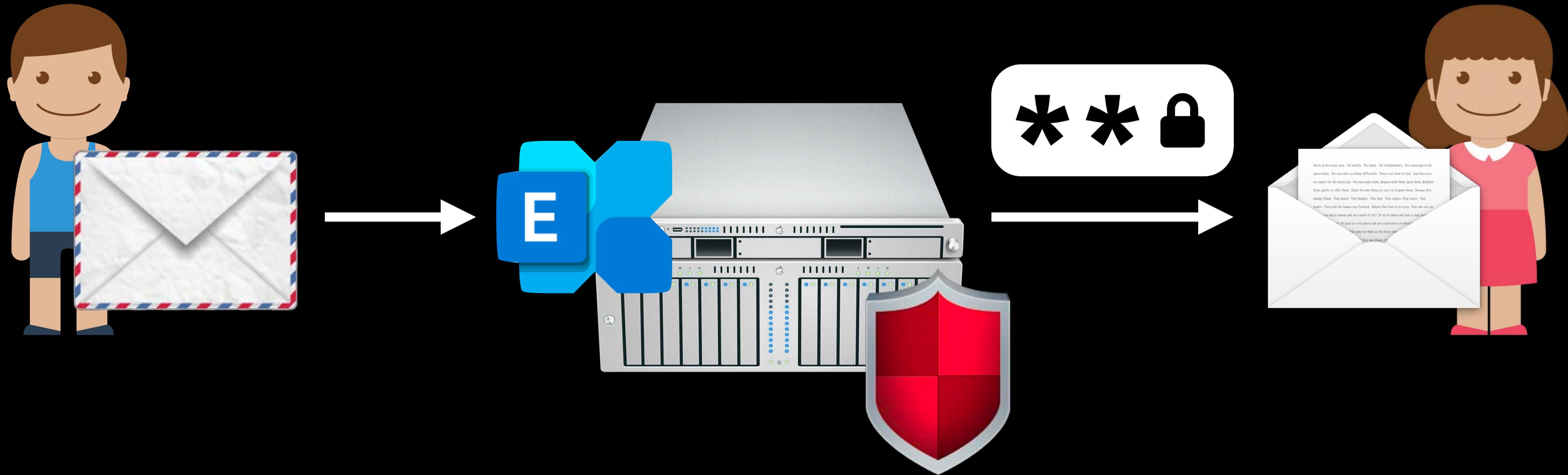




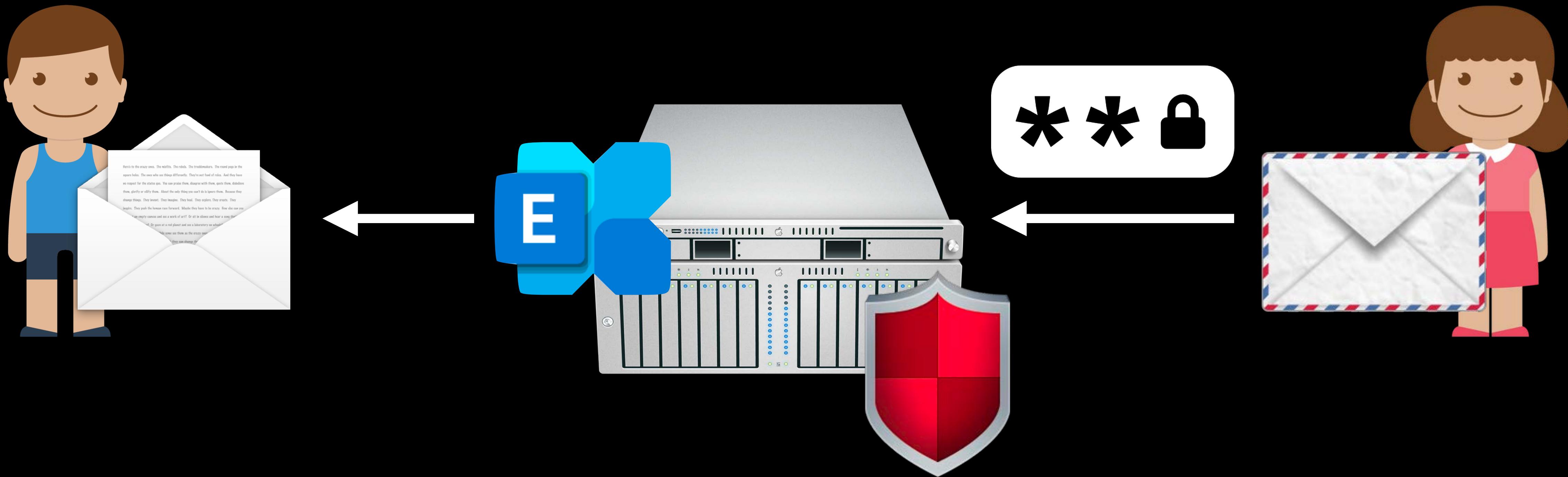
# THREAT HUNTING

Lessons Learned from our Journey to the Cloud

# TRADITIONAL EMAIL ARCHITECTURE



# TRADITIONAL EMAIL ARCHITECTURE

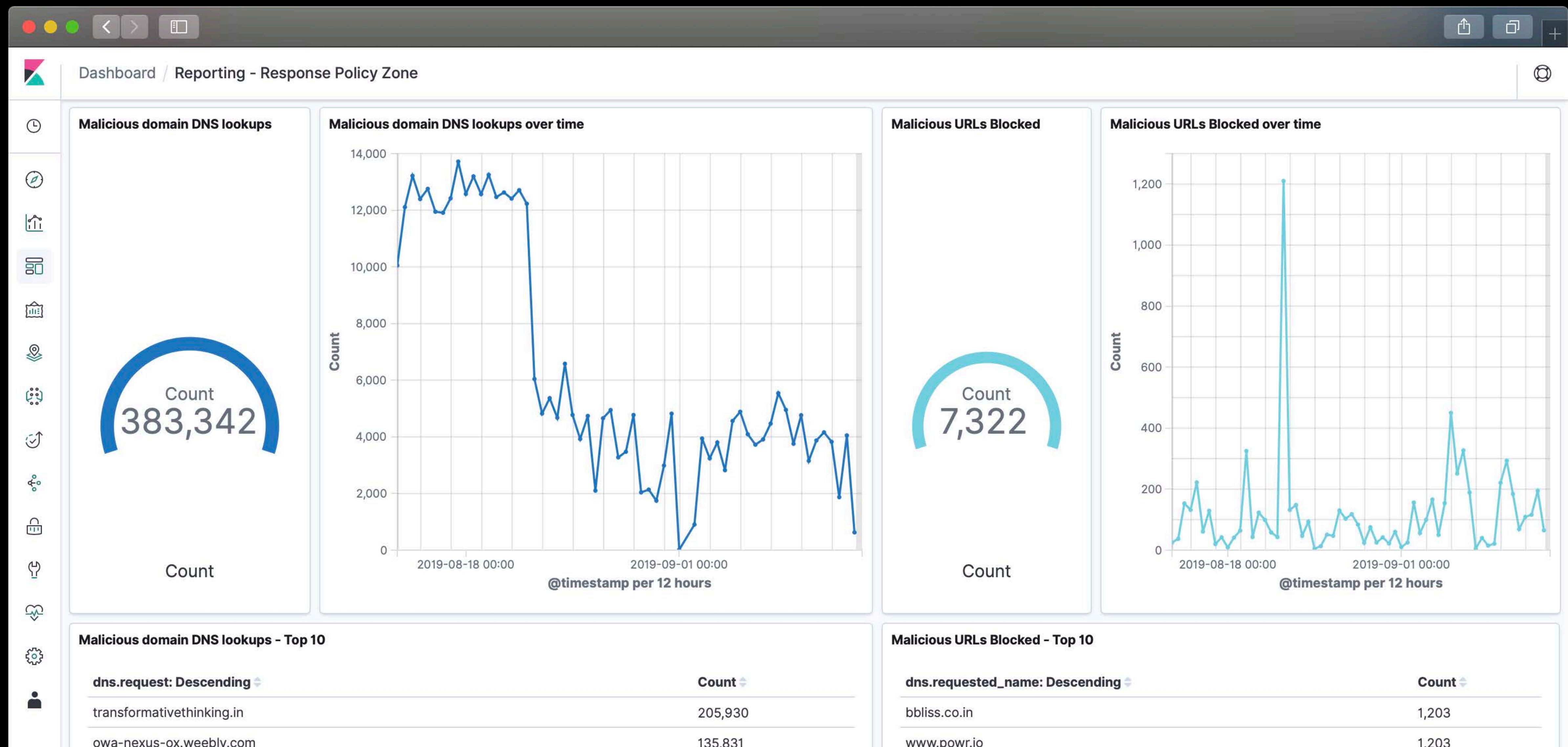




# REASONS FOR A CUSTOM RPZ



UNIVERSITY OF  
OXFORD



# STRATEGIES AGAINST PHISHING?



User education: training, awareness campaigns, internal phishing exercises.

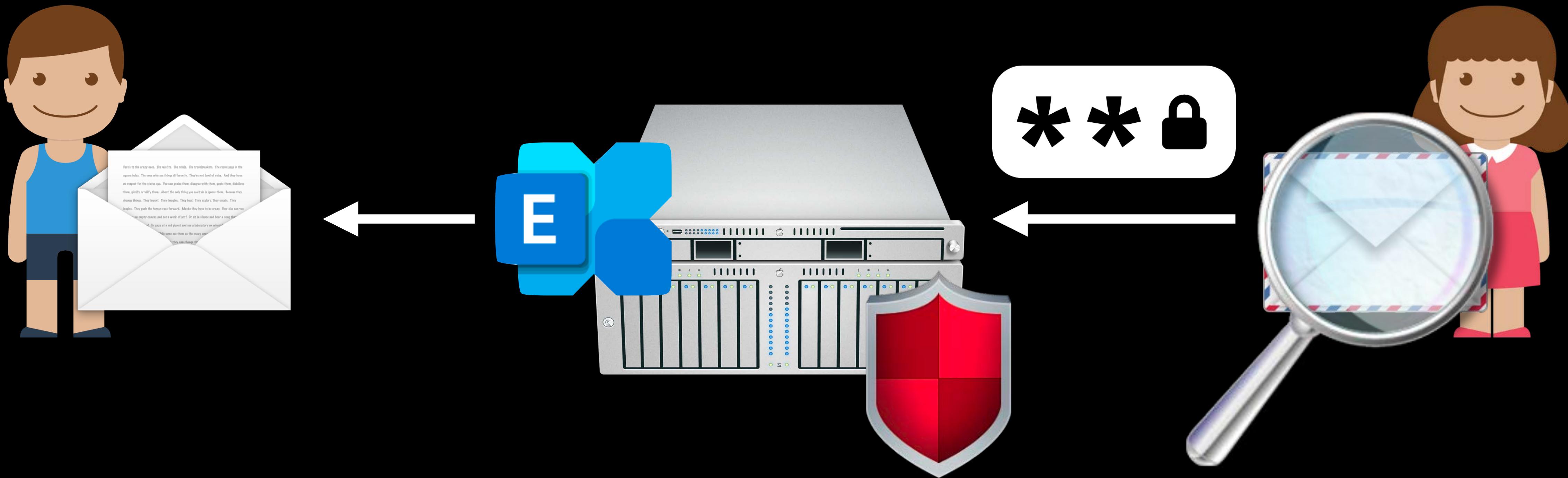
Email security products.

DNS Firewall (Response Policy Zone) to subvert phishing sites to a sinkhole.

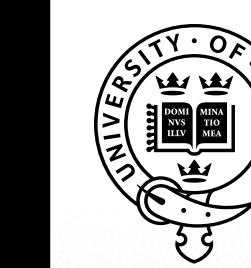
Endpoint web filtering using the RPZ.

# COMPROMISED ACCOUNTS BEHAVE ANOMALOUSLY

# COMPROMISED ACCOUNT DETECTION



# COMPROMISED ACCOUNT DETECTION



# UNIVERSITY OF OXFORD

The screenshot shows a terminal window with the following details:

- Title Bar:** The title bar displays the file name "detect\_spammer.pl".
- Toolbar:** The toolbar includes standard icons for file operations like "notify", "refresh", "copy", "paste", and "quit".
- Code Content:** The main area contains Perl code for a spammer detector. The code includes SVN metadata at the top and uses modules like Net::SMTP, Getopt::Long, Text::ParseWords, and Switch. It defines variables for disabled counts, mail from, and descriptions, and ends with a loop to process emails.

```
1 #!/usr/bin/perl
2 # $HeadURL:
3 # https://secret.oxcert.ox.ac.uk/svn/conf/rb3/systems/spam-detector.oxcert.ox.ac.uk/root/usr
4 # /local/bin/detect_spammer.pl $
5 # $LastChangedRevision: 29666 $
6 # $LastChangedDate: 2019-06-13 14:21:07 +0100 (Thu, 13 Jun 2019) $
7 # $LastChangedBy: horst $
8 #
9 # *** Generated from sources/usr/local/bin/detect_spammer.pl.tt ***
10 #
11 use strict;
12 use warnings;
13 use Net::SMTP;
14 use Getopt::Long;
15 use vars qw($opt_help $opt_debug);
16 use Text::ParseWords;
17 use Switch;
18 use POSIX qw(strftime);
19 my $disabled_first = 10;
20 my $disabled_rate = 10;
21 my $mail_from='[REDACTED]';
22 my $mail_desc='OxCERT Email Spammer Alert';
23 my $oxcert_email='[REDACTED]';
24 my @emails:[REDACTED]
```

# COMPROMISED ACCOUNT DETECTION



From: "0xCERT Email Spammer Alert" <detector@infosec.ox.ac.uk>  
To: detections@infosec.ox.ac.uk  
Subject: Possible Spammer alert - Rate limit exceeded: <help@it.ox.ac.uk>  
Date: Fri, 13 Sep 2019 13:13:13 +0100

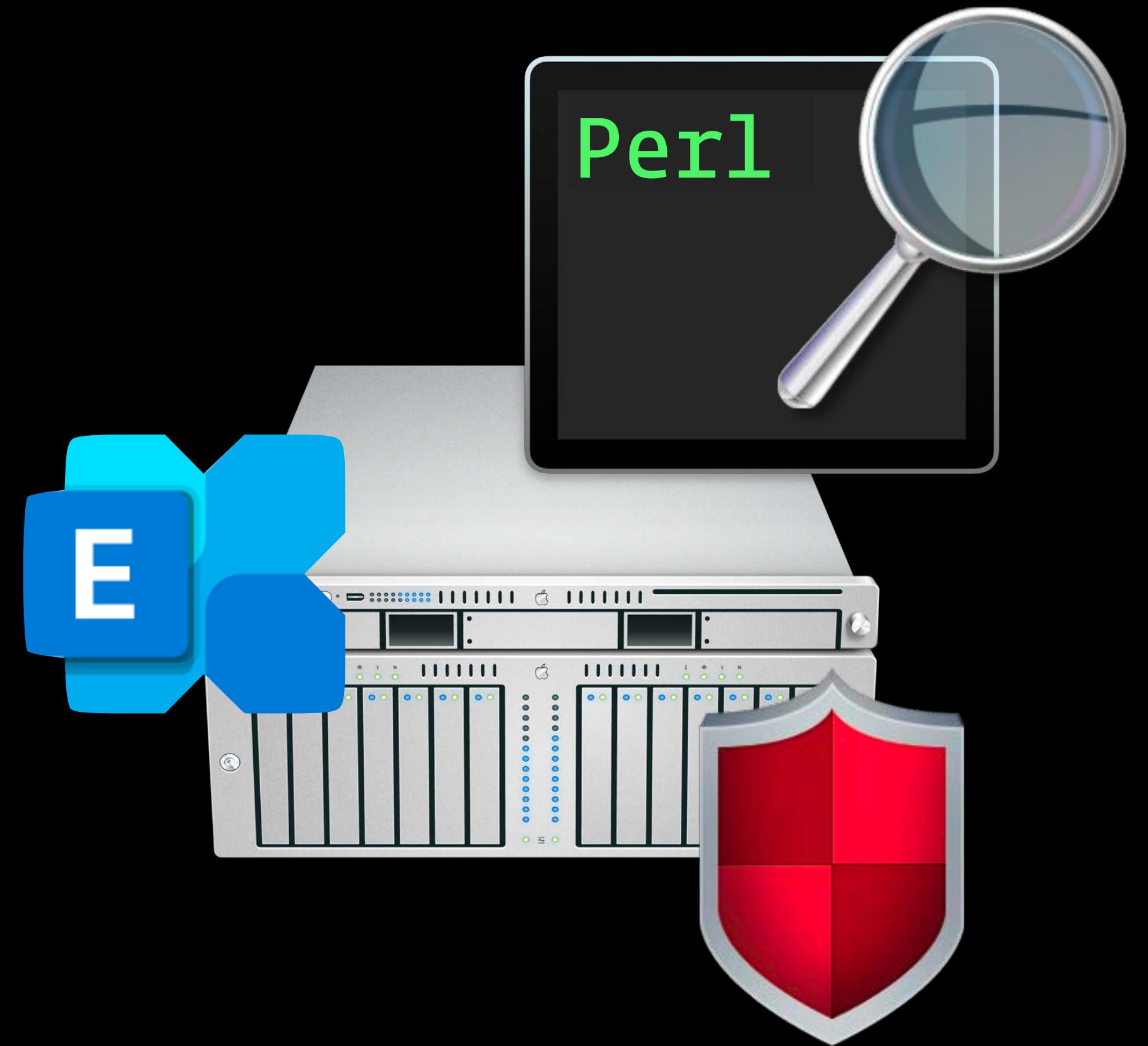
The following log entry was detected:

```
Sep 13 13:13:13 host exim[41679]: H=host.mail.ox.ac.uk [1.2.3.4]
X=TLS1.2:ECDHE_RSA_AES_256_GCM_SHA384:256 CV=no F=<help@it.ox.ac.uk>
temporarily rejected RCPT <random@hotmail.com>: SND-FLD help@it.ox.ac.uk
sender address limit exceeded to random@hotmail.com rate=n+1 ratelimit=n
```

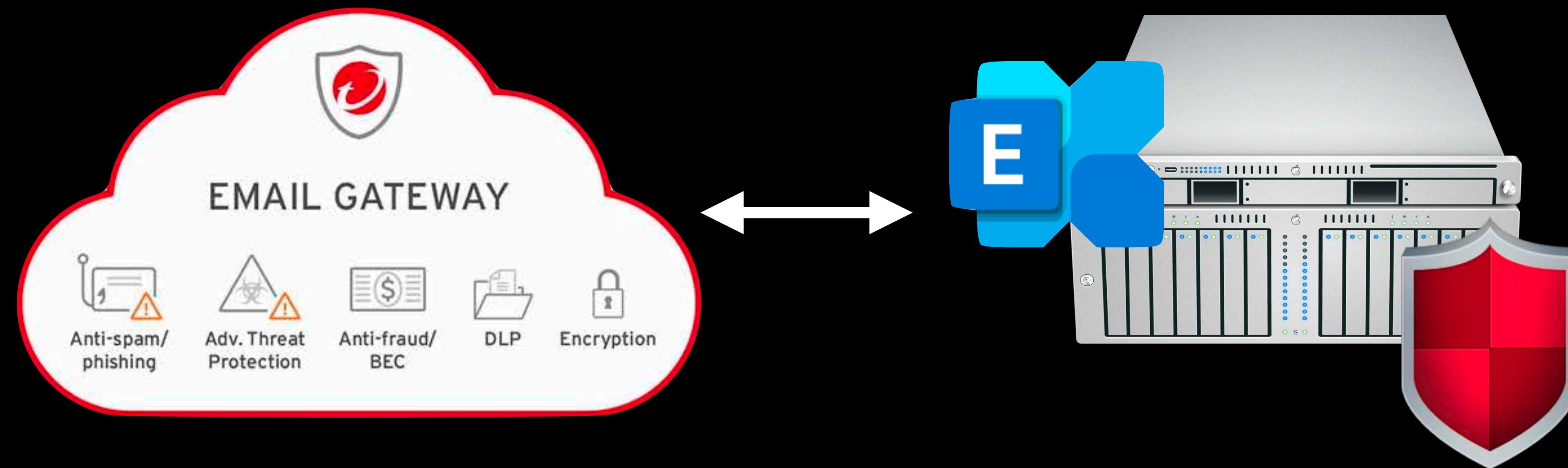
SSO username: **user1234**

FROM top subjects:

(1298) **Nexus Upgrade Message**



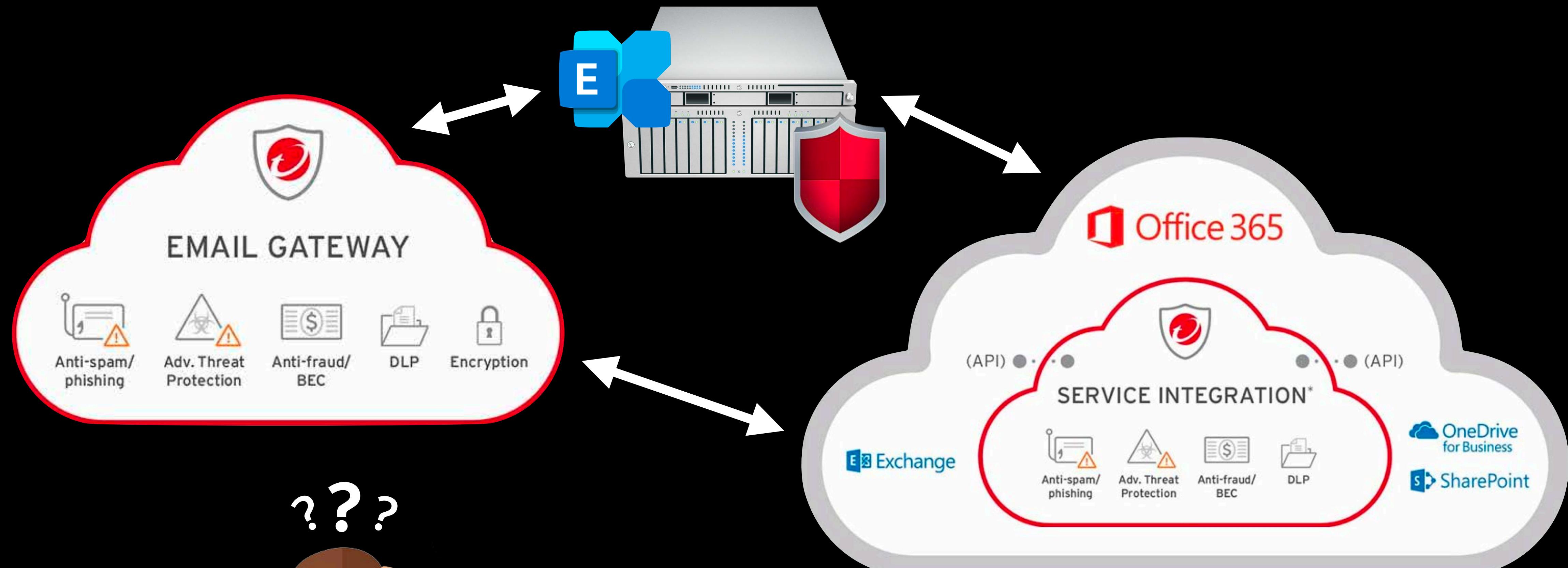
# EMAIL SECURITY AS A SERVICE



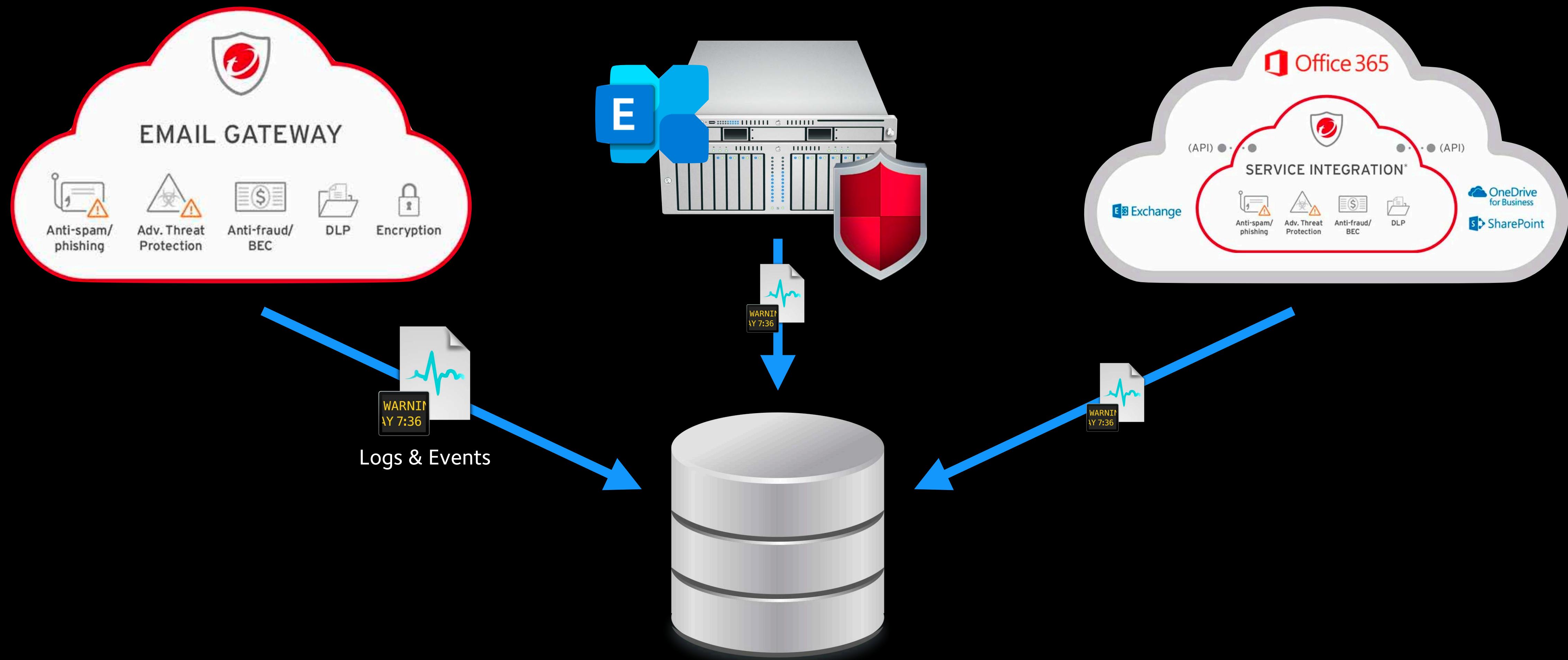
# HYBRID CLOUD



UNIVERSITY OF  
OXFORD



# HYBRID CLOUD SECURITY ANALYTICS





# **SIEM**

## Security Information and Event Management



# **SIEM+**

Entity and User Behaviour Analytics  
Security Orchestration, Automation and Response  
Threat Intel Retro-Matching

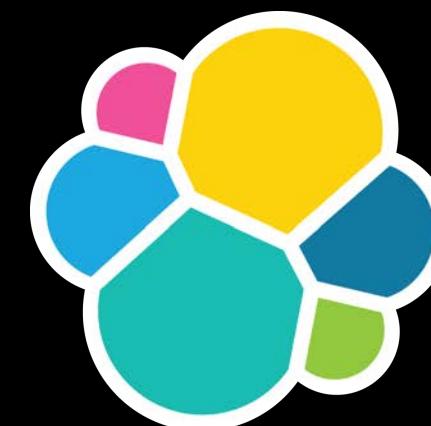
# THE TOOL MAKETH THE TEAM



SIEM+



SIRT



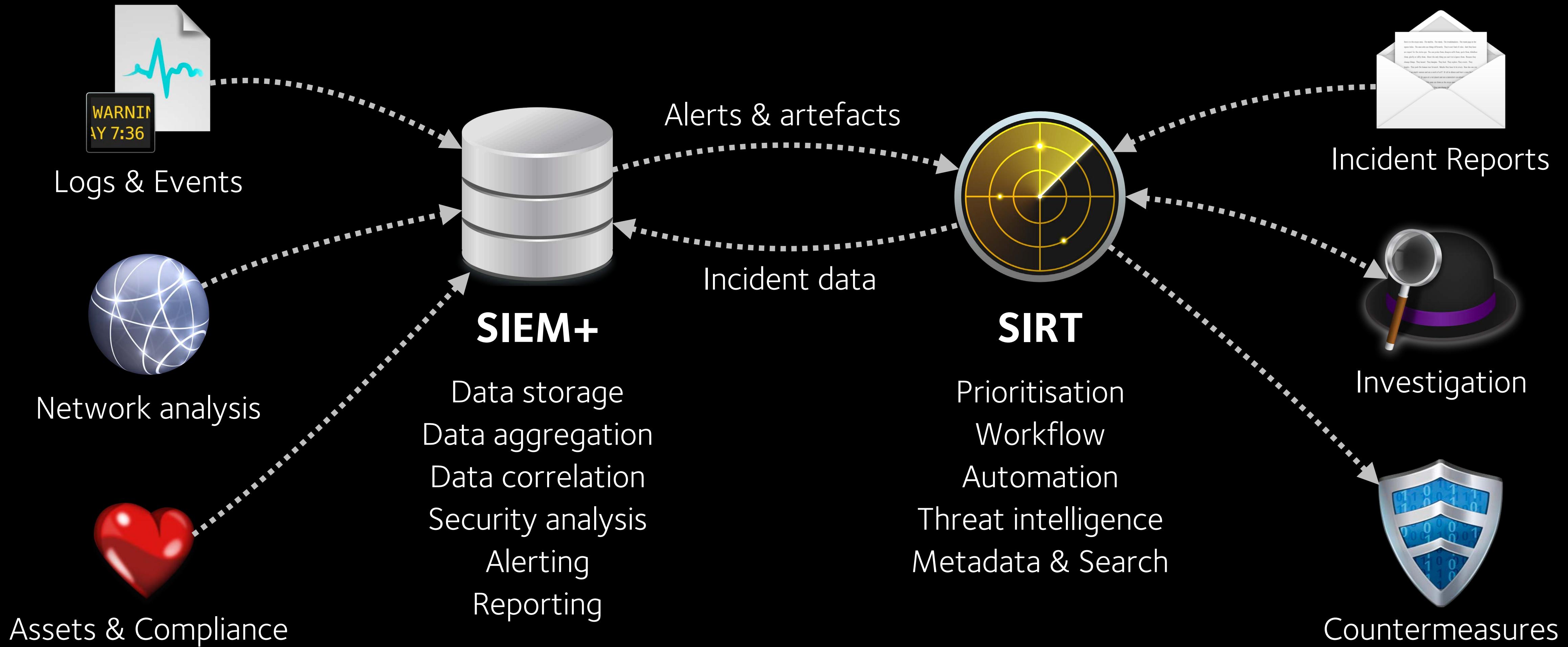
elastic

<https://elastic.co>

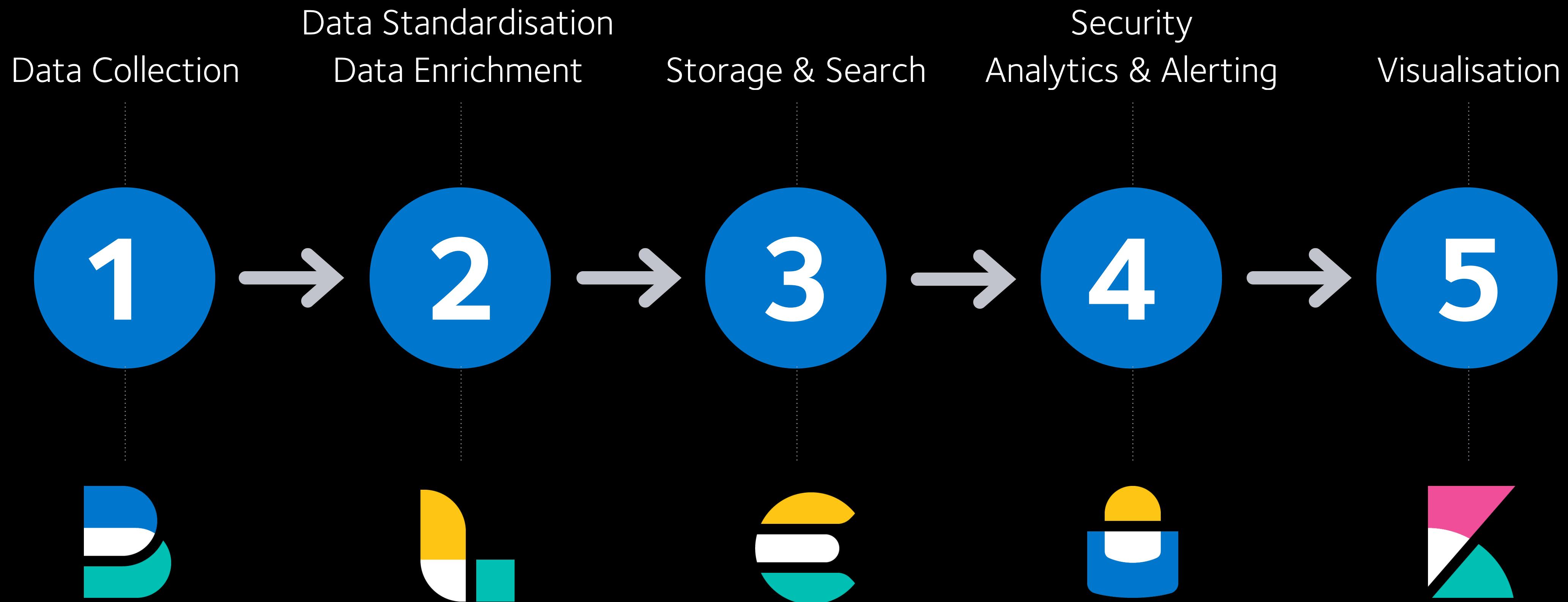
>< BEST  
PRACTICAL™

<https://bestpractical.com/rtir/>

# THE TOOL MAKETH THE TEAM



# ELASTIC STACK IN A NUTSHELL



# GET A HANDLE ON YOUR DATA



Just collecting all possible logs, events, and alarms does not help making sense out of them!

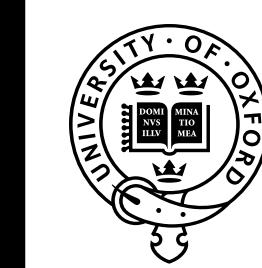
- NTP time source, UTC based logging, and ISO 8601 date
- Normalise your data during ingest

e.g. 2001:420:1101:1::A vs 2001:420:1101:1:0:0:0:a

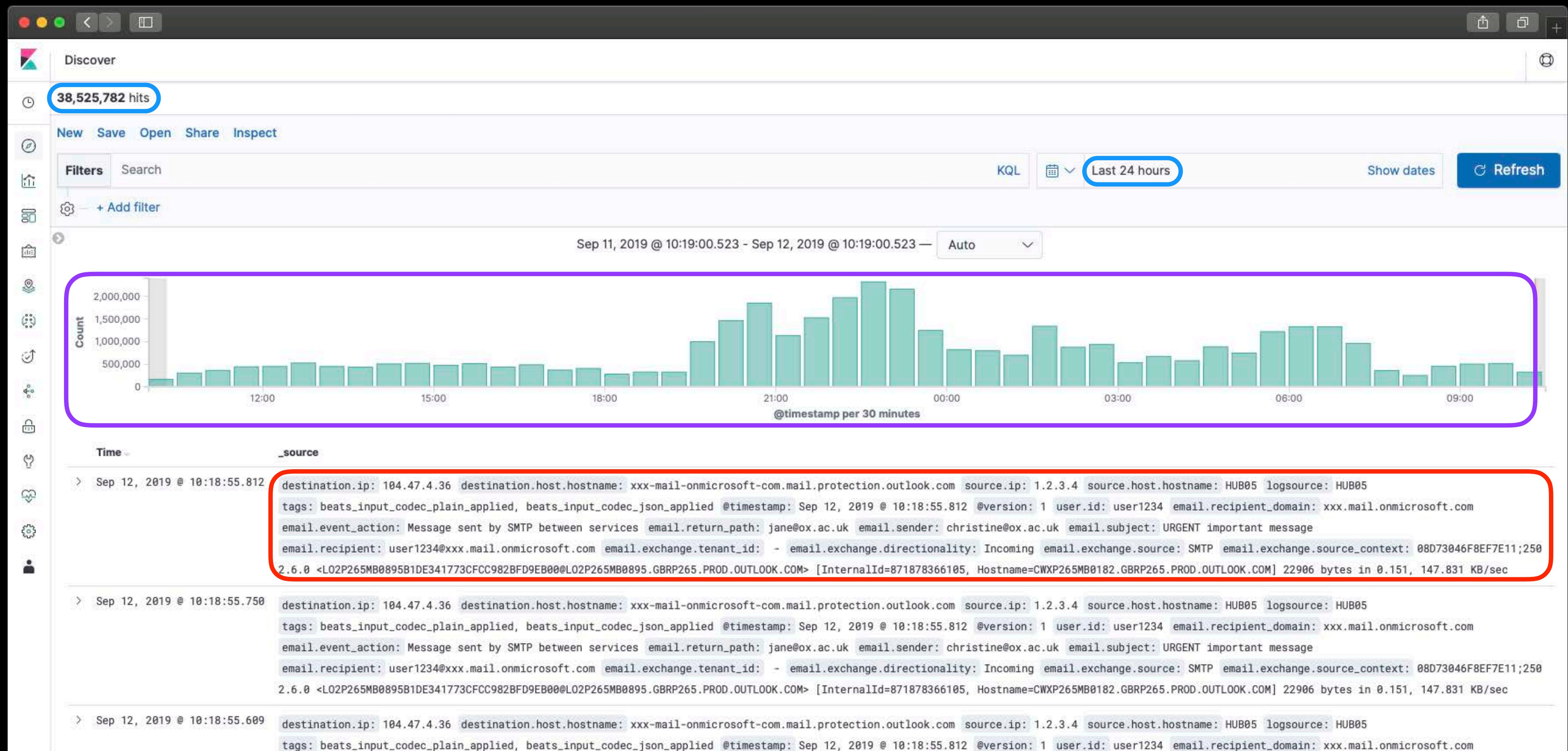
- Enrich during ingest and continuously curate metadata
- Use a consistent schema (*Elastic Common Schema*)
- Keep just the facts – filter and prepare your data



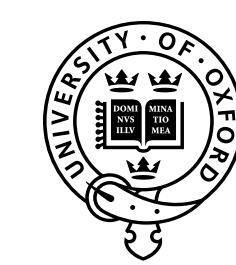
# DATA DISCOVERY USING ELASTIC



UNIVERSITY OF  
OXFORD



# DASHBOARDS USING ELASTIC



UNIVERSITY OF  
OXFORD

Dashboard / SMTP

Full screen Share Clone Edit

Filters 2 Search

NOT error.message exists × NOT Common mass mailers × + Add filter

smtp user

smtp Source Hostname

smtp Unusual terms in subject

Navigation

Mail | VPN

OXMAIL ratelimit

email.sender: Descending	Count
help@it.ox.ac.uk	4,249,566
[REDACTED]	3,401,556
[REDACTED]	2,251,852
[REDACTED]	2,268

SMTP subjects

Subject	Count
Mail delivery failed: returning message to sender	8,680
Cron www-data@clashelp /usr/bin/php5 /usr/share/glpi/front/cron.php	1,440
Resolved: Unavailable by ICMP ping	615
[REDACTED]	591
[REDACTED]	576
p_cir_12 Success	528
Attached Image	491
[REDACTED]	477
[REDACTED]	474
Missing host in proxy	421

smtp sender

Sender	Count
help@it.ox.ac.uk	28,582
[REDACTED]	28,542
[REDACTED]	9,016
[REDACTED]	8,525
[REDACTED]	6,085
[REDACTED]	5,910

# THE RISE OF THE MACHINES

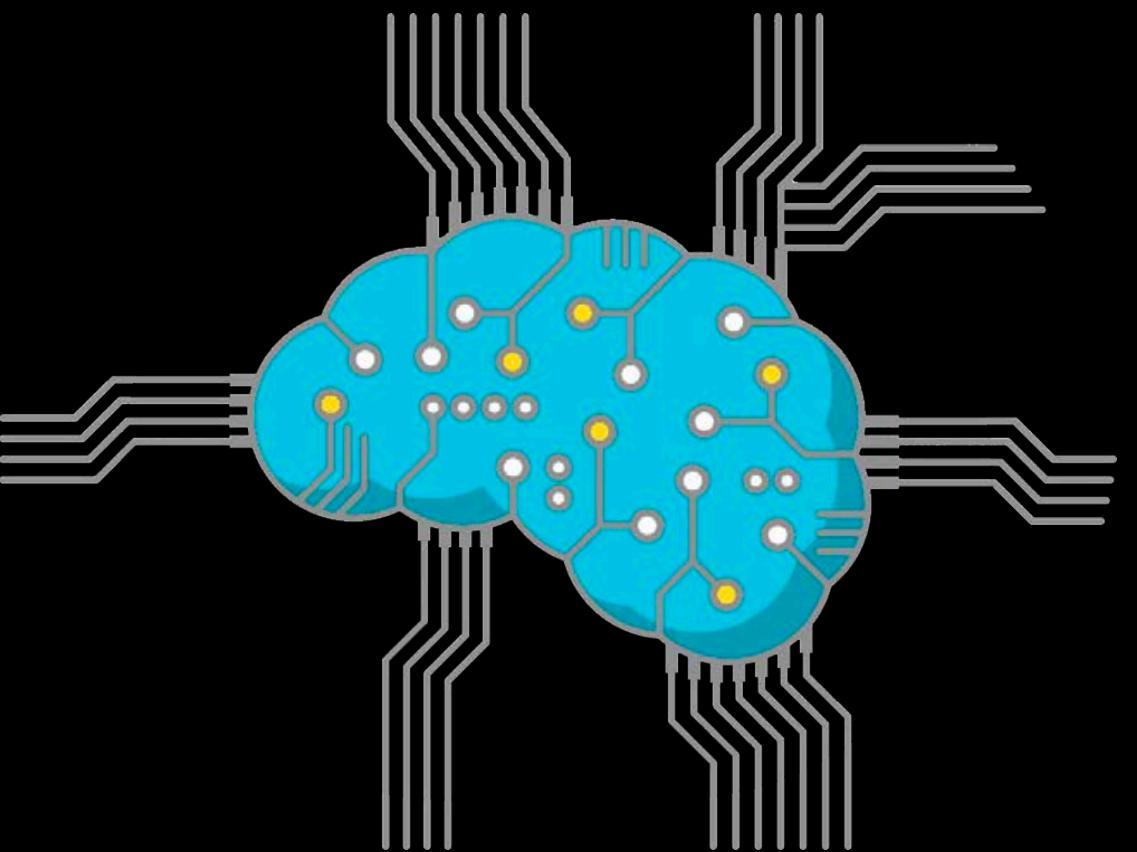
# WHAT IS MACHINE LEARNING?



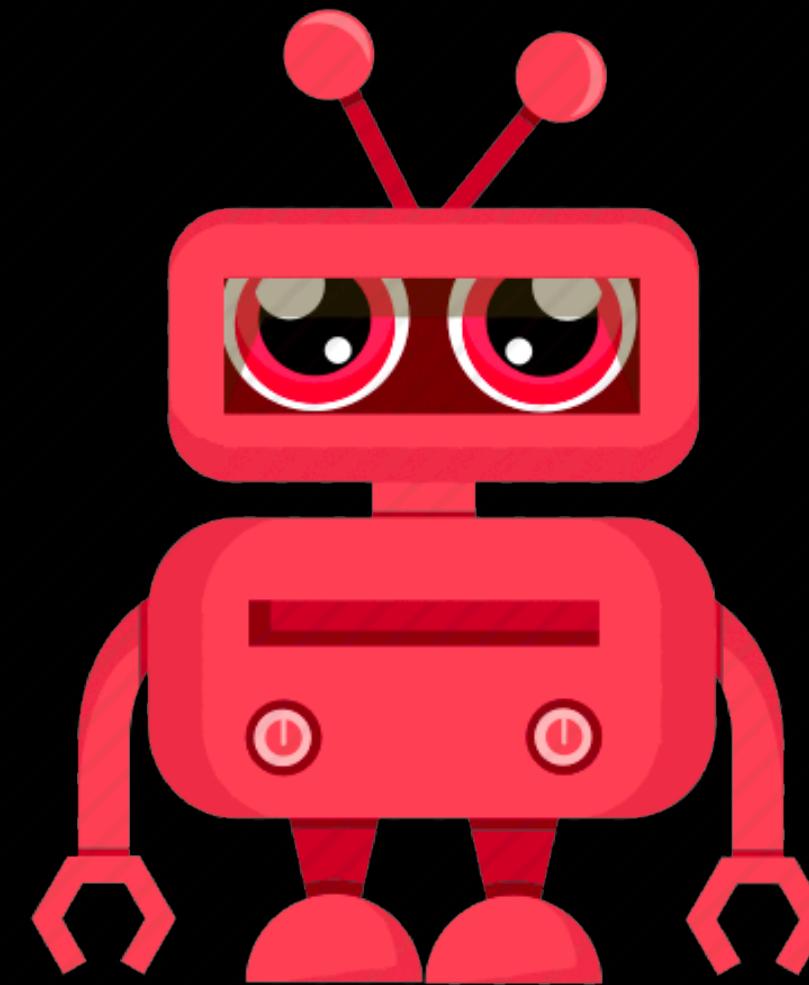
Learn from experience



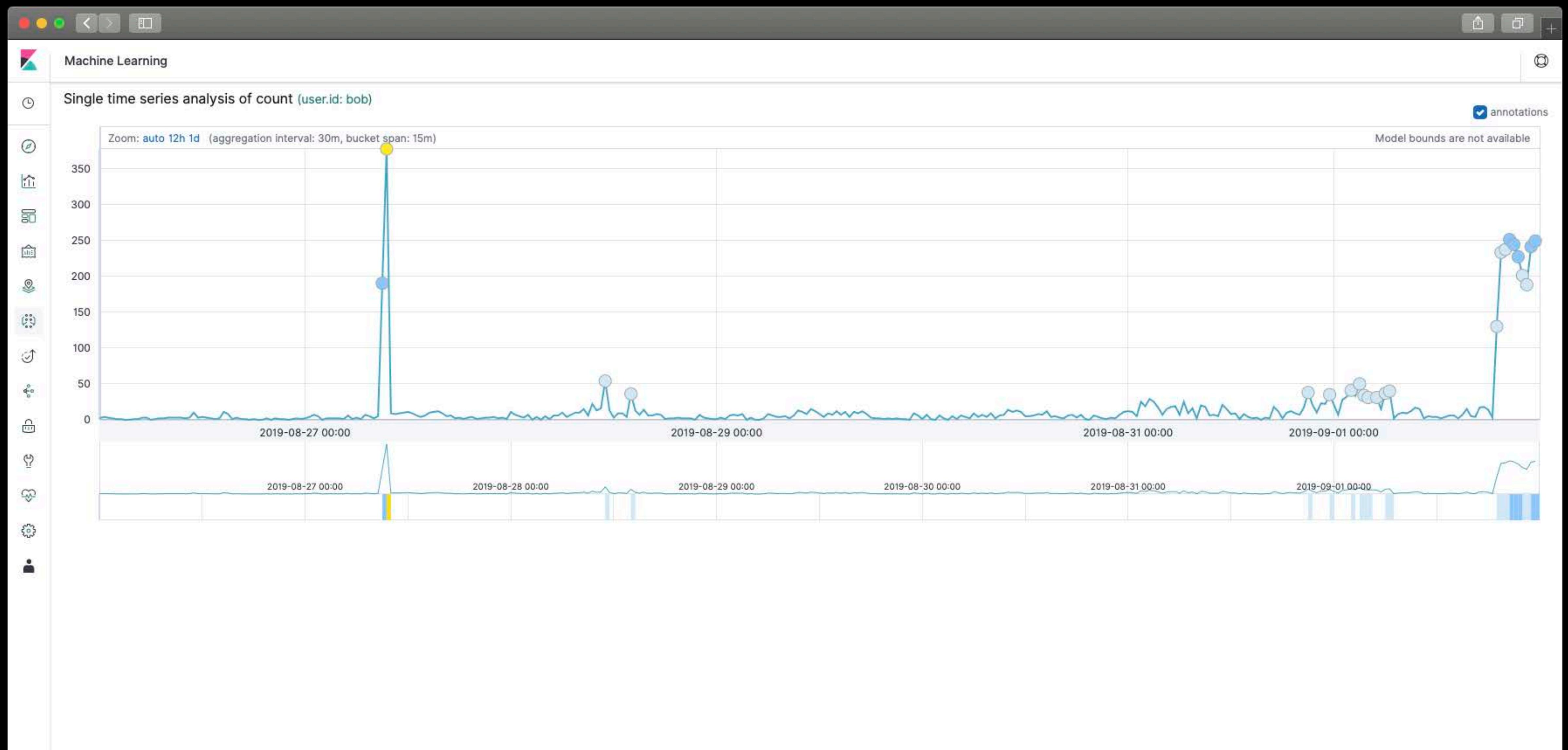
Learn from ~~experience~~ **data**?



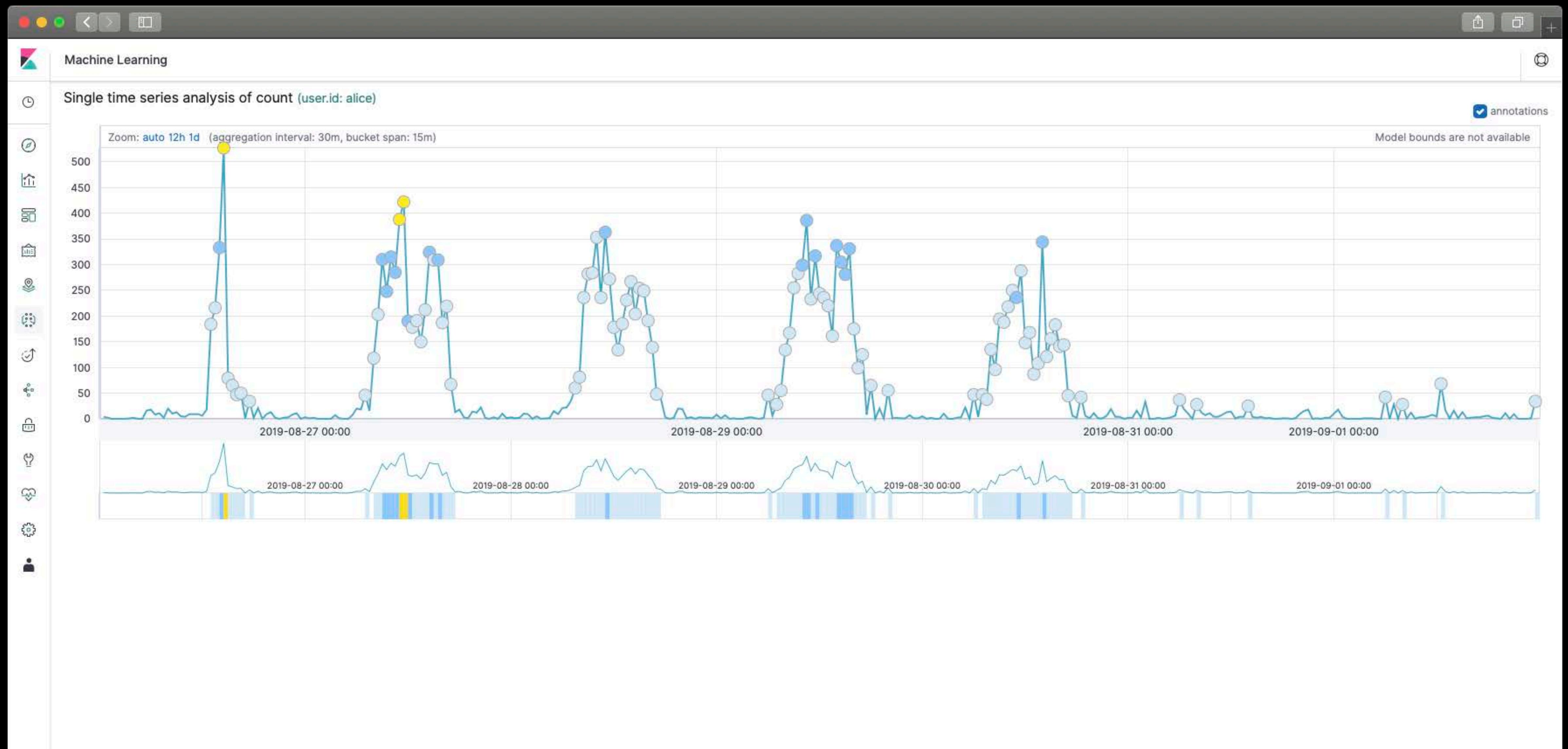
Follow instructions



# NOT ALL ENTITIES ARE THE SAME



# NOT ALL ENTITIES ARE THE SAME



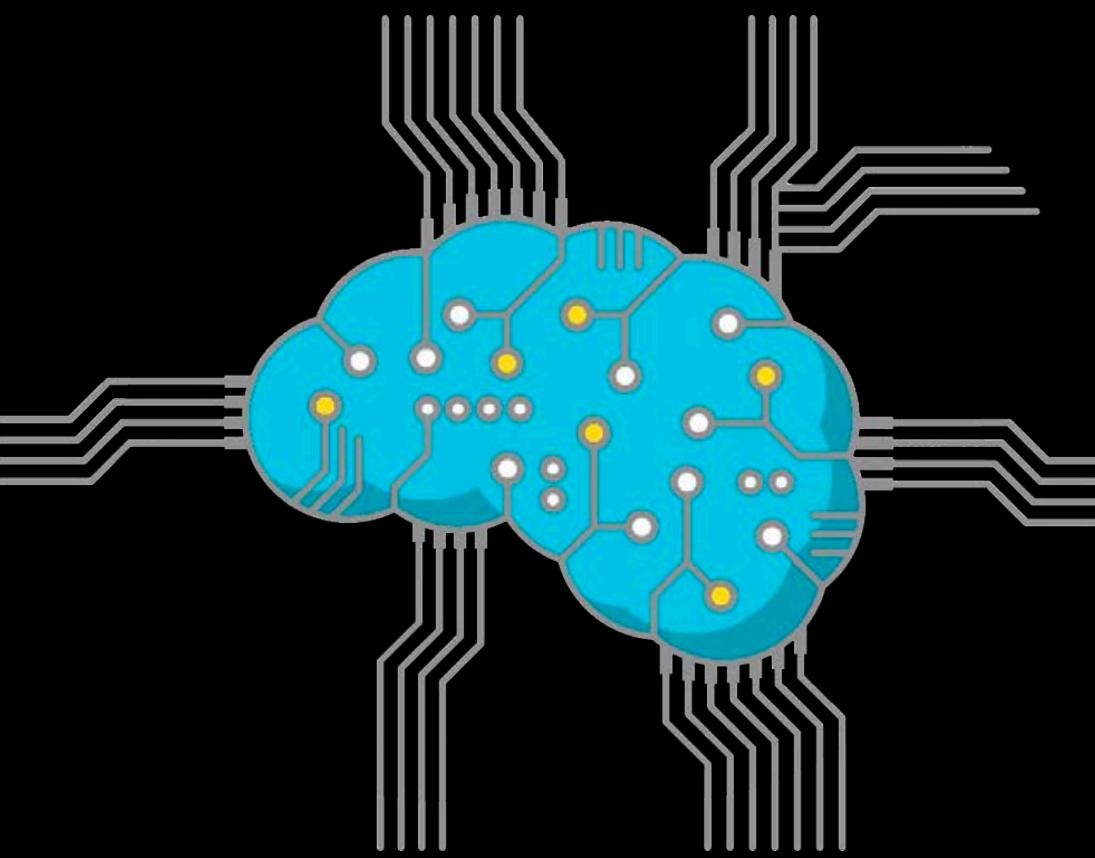
# TIME SERIES ANALYSIS



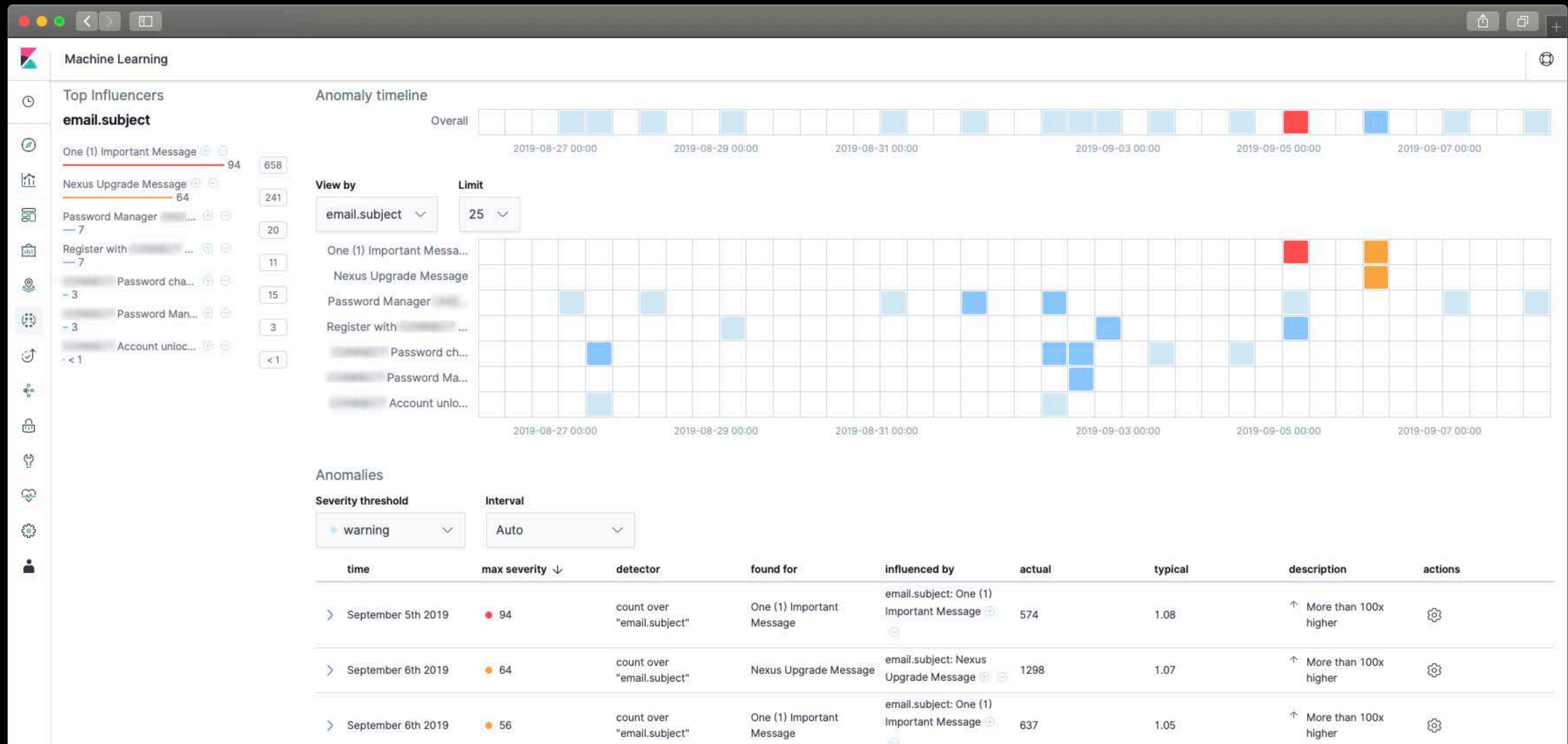
Security Analyst's experience



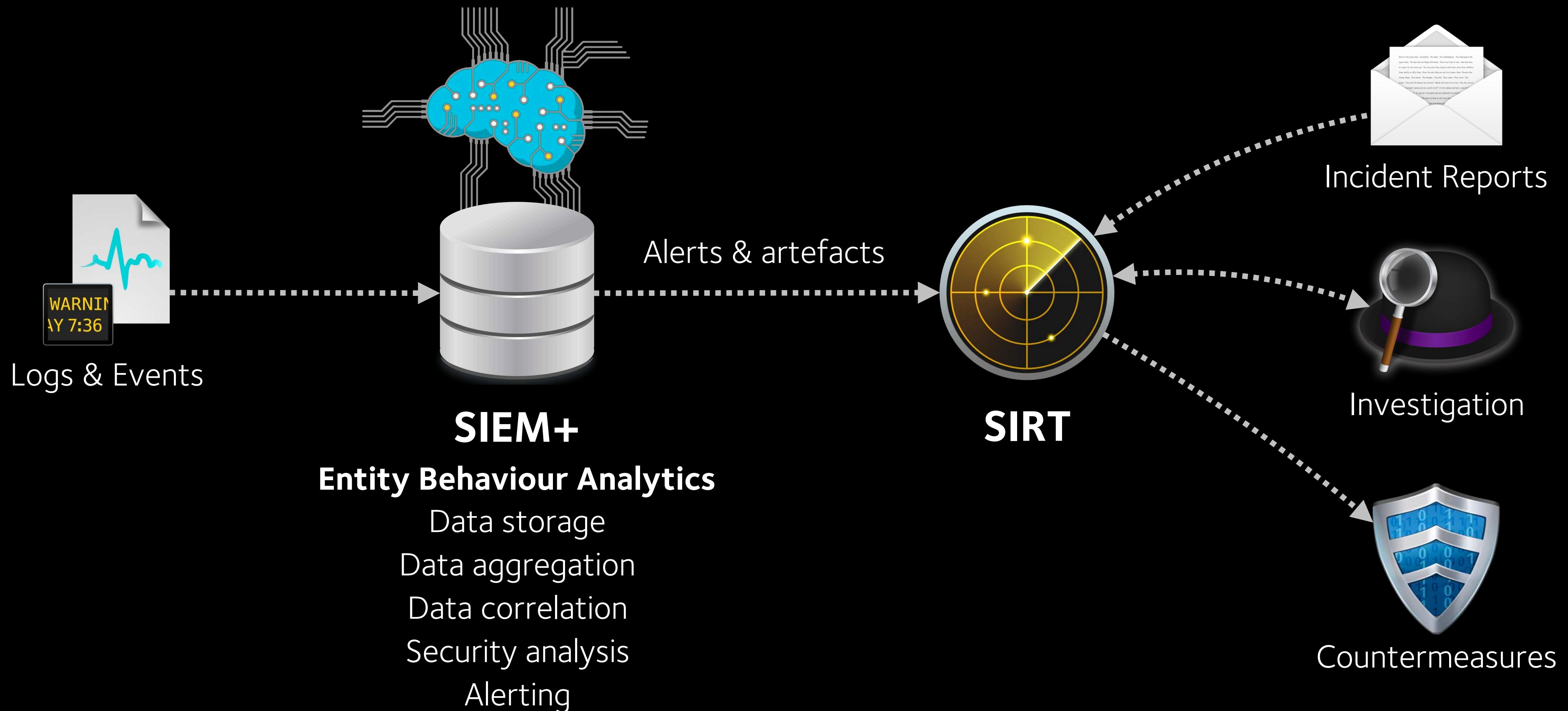
Unbiased evidence in data



# ANOMALY TIMELINE FOR ONE ENTITY



# SIEM+ GOT A LITTLE SMARTER





# SIEM+

Entity and User Behaviour Analytics ✓  
Security Orchestration, Automation and Response  
Threat Intel Retro-Matching

# FUTURE: AUTOMATED COUNTERMEASURES



Online Help Center

Home / Enterprise / Cloud App Security Integration API Online Help

Privacy and Personal Data Collection Disclosure

Getting Started with Cloud App Security Automation and Integration APIs

Supported Cloud App Security Automation APIs

- Log Retrieval API
- Threat Investigation API
- Threat Mitigation APIs

API Responses

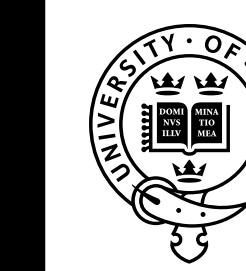
## Supported Cloud App Security Automation APIs

This section discusses the following supported Cloud App Security Automation APIs.

API Type	Actions	Description
Log retrieval	Get security logs	Retrieves security event logs of the services that Cloud App Security protects
Threat investigation	Sweep for email messages	Searches email messages in protected mailboxes for those that match meta information search criteria
Threat mitigation	Take actions on user accounts Take actions on email messages Query action results	Takes actions on a batch of specified user accounts Takes actions on a batch of specified email messages Queries the results of actions on specified email messages or user accounts

[Log Retrieval API](#)  
[Threat Investigation API](#)  
[Threat Mitigation APIs](#)

# FUTURE: AUTOMATED COUNTERMEASURES



UNIVERSITY OF  
OXFORD

Not Secure — docs.trendmicro.com/en-us/enterprise/cloud-app-security-integration-api-online-help/su...

## Sweep for Email Messages

Searches email messages in Cloud App Security protected mailboxes for those that match meta information search criteria.

### HTTPS Request

```
GET https://<serviceURL>/v1/sweeping-mails
```

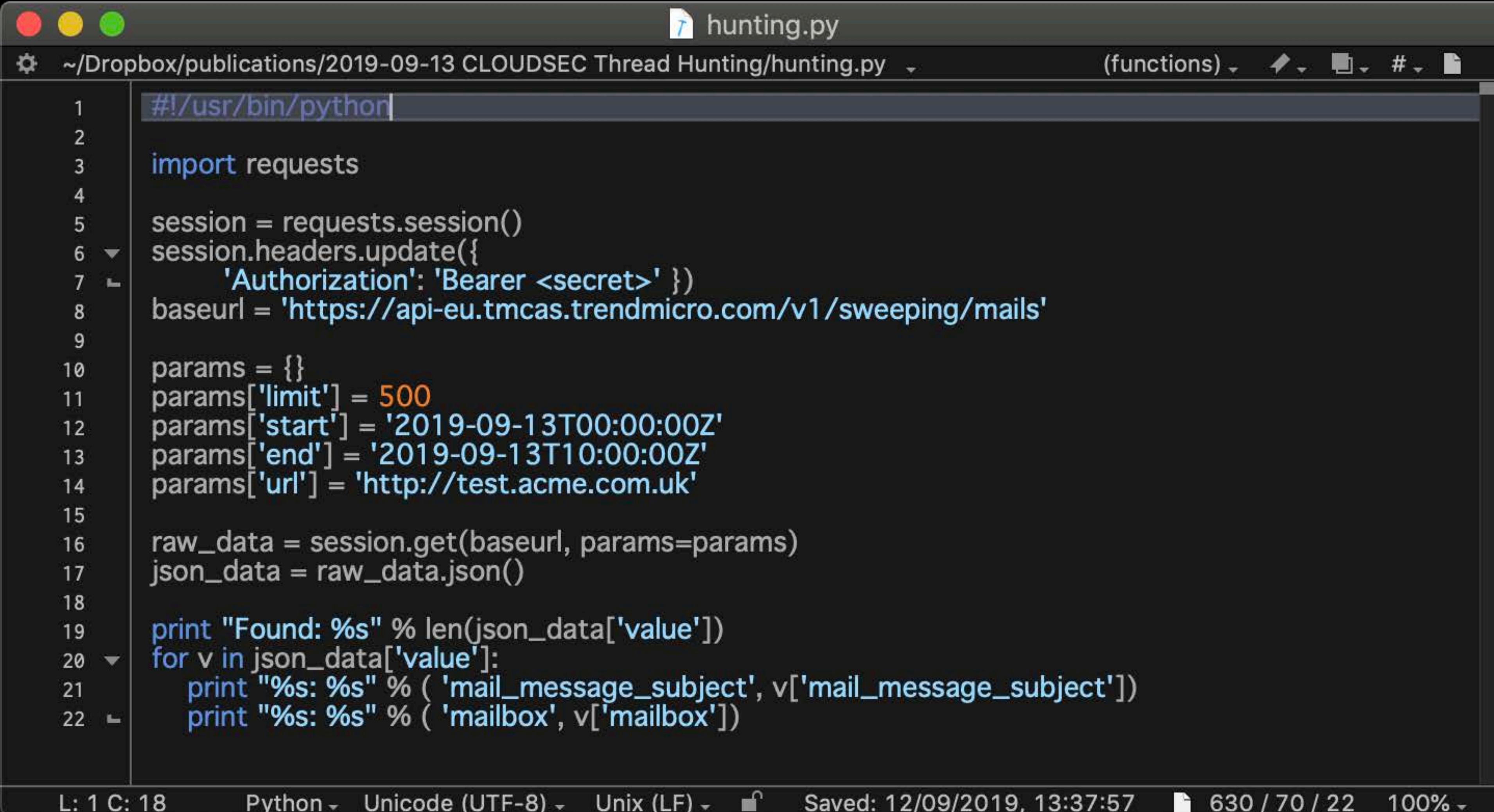
### Request Parameters

Parameter	Description
mailbox	Email address of the mailbox to search in Type a complete email address. Non-prefix wildcard is supported. Example: u*ser@example.com or user@ex*ample.com
start	Start and end time during which email message are to search. Format: ISO 8601 timestamp to the second or millisecond in UTC, <b>yyyy-mm-ddThh:mm:ss[.mmm]Z</b> . For example, <b>2016-07-22T01:51:31Z</b> or <b>2016-07-22T01:51:31.001Z</b> .
end	Cloud App Security saves the meta information of email messages for 90 days. The request searches email messages according to the start and end settings: <ul style="list-style-type: none"><li>If both start and end are not specified, the request searches email messages within seven days (7 × 24 hours) before the point of time when the request is sent.</li><li>If both start and end are specified, the request searches email messages within the configured duration. Make sure the <b>end</b> time is no earlier than the <b>start</b> time.</li><li>If only start is specified, the request searches email messages within seven days (7 × 24 hours) after the point of the configured <b>start</b> time.</li><li>If only end is specified, the request searches email messages within seven days (7 × 24 hours) before the point of the configured <b>end</b> time.</li></ul> <p>Do not configure lastdays and start/end at the same time.</p>
subject	Subject of email messages to search for If you set the value to <b>A B</b> , Cloud App Security searches for email messages whose subject contains <b>A</b> , or <b>B</b> , or <b>A B</b> . To search for an exact phrase, for example, <b>A B</b> , enclose the value in double quotes " <b>A B</b> ".

# PROOF OF CONCEPT CODE



UNIVERSITY OF  
OXFORD



A screenshot of a code editor window titled "hunting.py". The file path is shown as "~Dropbox/publications/2019-09-13 CLOUDSEC Thread Hunting/hunting.py". The code itself is a Python script for thread hunting, utilizing the requests library to interact with a Trend Micro API endpoint. The script defines parameters for the API call, including a limit of 500 items, a start date of 2019-09-13T00:00:00Z, an end date of 2019-09-13T10:00:00Z, and a specific URL. It then prints the length of the JSON data and iterates through each item to print the mail message subject and mailbox.

```
#!/usr/bin/python

import requests

session = requests.Session()
session.headers.update({
    'Authorization': 'Bearer <secret>' })
baseurl = 'https://api-eu.tmcas.trendmicro.com/v1/sweeping-mails'

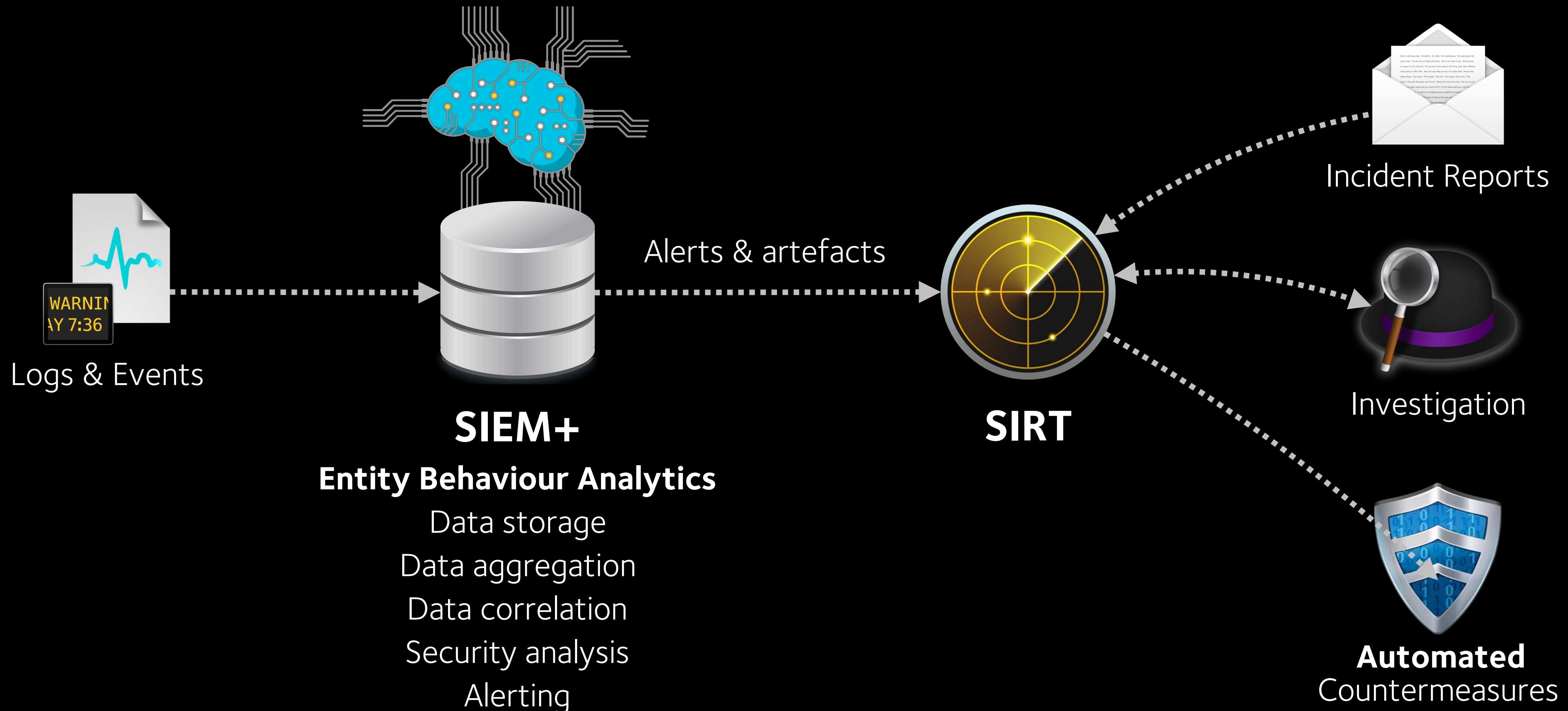
params = {}
params['limit'] = 500
params['start'] = '2019-09-13T00:00:00Z'
params['end'] = '2019-09-13T10:00:00Z'
params['url'] = 'http://test.acme.com.uk'

raw_data = session.get(baseurl, params=params)
json_data = raw_data.json()

print "Found: %s" % len(json_data['value'])
for v in json_data['value']:
    print "%s: %s" % ( 'mail_message_subject', v['mail_message_subject'])
    print "%s: %s" % ( 'mailbox', v['mailbox'])
```

L: 1 C: 18    Python ▾  Unicode (UTF-8) ▾  Unix (LF) ▾  Saved: 12/09/2019, 13:37:57    630 / 70 / 22    100% ▾

# SIEM+ GOT EVEN MORE SMARTER





# SIEM+

Entity and User Behaviour Analytics ✓

Security Orchestration, Automation and Response ✓

Threat Intel Retro-Matching

DATA-DRIVEN

MULTI-VENDOR

APIs

AUTOMATION

AGILITY

BIG DATA

# SECDEVOPS

ORCHESTRATION

VELOCITY

INTEGRATION

PERMISSIVE CULTURE

RETRO MATCHING AND HUNTING

ADAPTABILITY





# THANK YOU!

**AARON WILSON**  
LINUX SECURITY LEAD

**MARKO JUNG**  
GLOBAL HEAD OF INFORMATION SECURITY OPERATIONS



[m@mju.ng](mailto:m@mju.ng)



[@mjung](https://twitter.com/mjung)



[fb.com/markohjung](https://fb.com/markohjung)